

Transformation

Striking the balance: Enhancing eCommerce fraud risk management for revenue growth

May 2024



Contents

1 Executive Summary

2 Introduction by Forter

3 Understanding the complex nature of eCommerce fraud

4 Effective fraud risk management for online merchants

5 Optimising fraud risk management practices

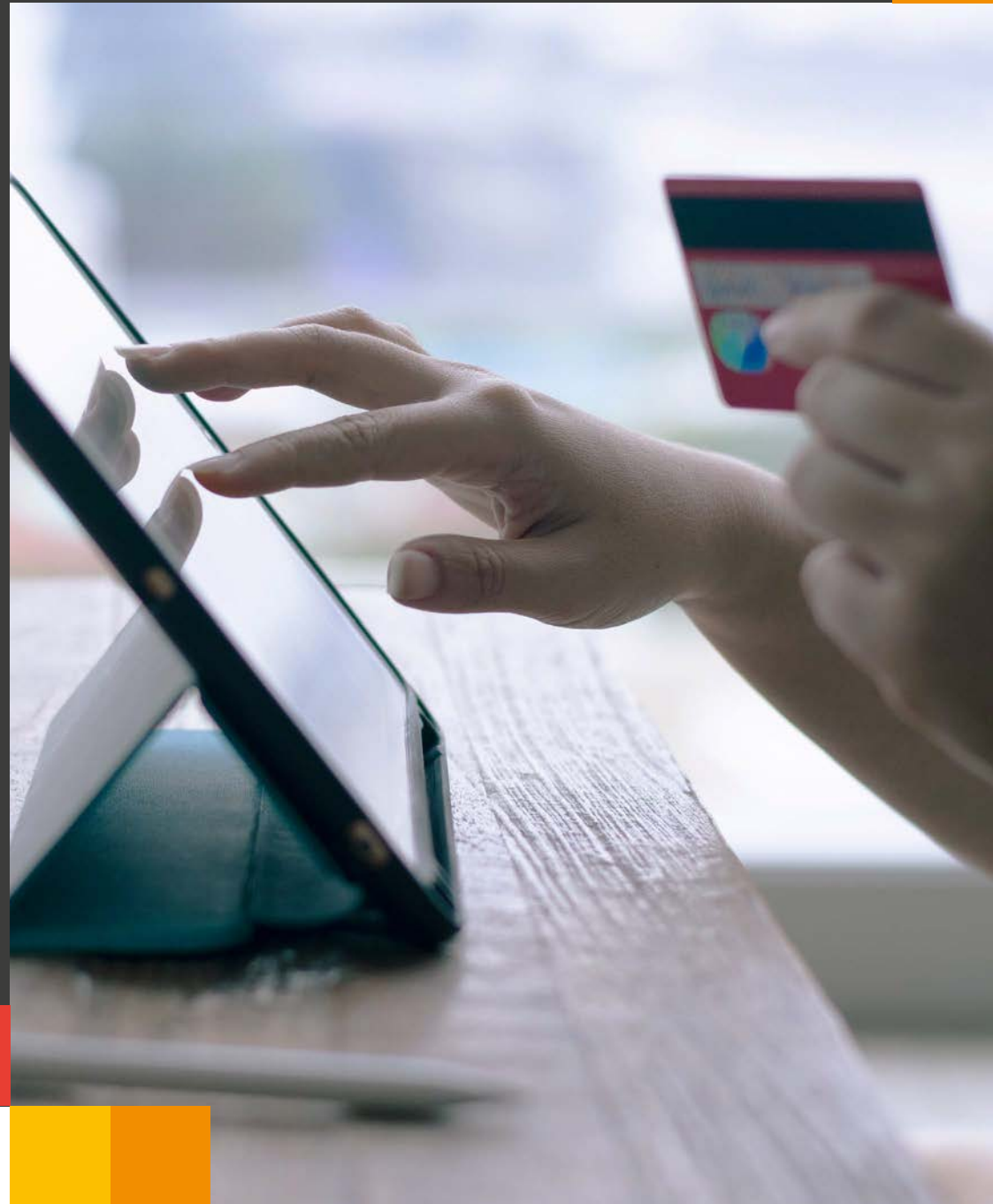
6 Considerations for the industry

7 PwC contact details

Executive Summary

Fraud is a ubiquitous and growing problem for online merchants. Fraud threats are becoming more diverse and complex, and merchant responses need to be increasingly nuanced and sophisticated to effectively balance fraud prevention with good customer experience and long term sales performance. Getting the balance wrong risks incurring heavy fraud losses and significant detriment to revenue.

Unfortunately, there is no simple solution to this complex problem and to make matters worse, the nature of the problem is changing all the time as customer behaviours and expectations evolve, new products and payment options are introduced and as new technologies become available to both merchants and fraudsters alike. In this context, agile and flexible fraud risk management strategies are required that can adapt to changing circumstances and prevent new fraud threat types getting out of hand. The foundation of such an agile approach is good data and in this paper we explore the hidden costs of ineffective fraud risk management approaches but also the benefits that can be derived from adopting more agile, data-driven approaches.



Just as data is the key for merchants to tackle fraud effectively, data is key to understanding the nature and scale of fraud threats and the potential benefits that can be delivered through effective fraud risk management. That's why we've partnered with Forter to develop this paper, bringing together their data-driven insights into fraud patterns and trends with our experience working with online merchants across the industry to tackle fraud related problems.

In this paper we show how effective fraud risk management can be a catalyst for revenue protection, encouraging merchants to consider fraud not just through the lens of direct fraud losses and chargeback prevention, but taking a broader view encompassing customer experience, sales conversion and the reduction of false declines. Understanding all of these factors when calibrating fraud risk management approaches has the potential to boost profitability at a time when customer spending remains tight and merchants are looking for ways to reduce costs.

We set out case studies where leading merchants have developed data analytics capabilities to analyse customer journeys, allowing them to monitor and optimise the effectiveness of their controls. The case studies also include examples of merchants that have adopted new technologies, like those provided by Forter, which offer greater potential for automation and reduce reliance on specialists to analyse data and spot trends.

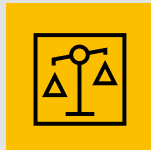


Key messages



eCommerce fraud is a dynamic and rapidly evolving threat

Merchants need to understand the breadth of fraud risks they face and implement strategies that are able to respond quickly, and proportionately, to changing threats. For larger merchants and merchants where sales are significantly concentrated in peak shopping periods like Black Friday and Christmas, automated fraud risk management approaches are critical to managing volumes and avoiding backlogs.



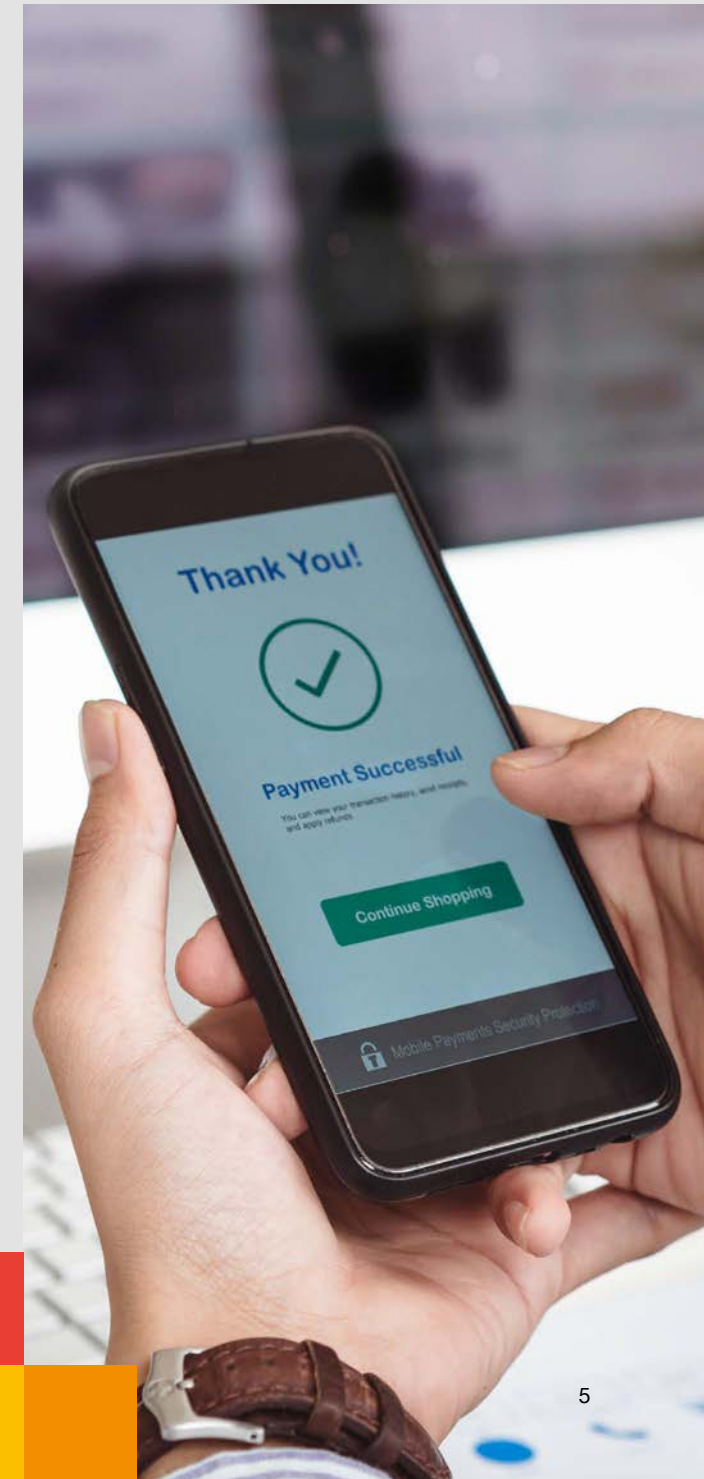
Effective fraud risk management requires a balancing act

To deliver effective fraud risk management, merchants must balance providing a good customer experience, preventing fraud, minimising operational costs of fraud prevention and driving high sales conversions. Getting the balance wrong with an ineffective fraud risk management approach can lead to high hidden costs driven by cart abandonment and false declines. These hidden costs can far outweigh apparent direct fraud losses and costs of fraud prevention but are often not measured effectively. Good data is critical to understanding and measuring success across each element of the balancing act and to enabling informed decision making.



Optimising fraud risk management can deliver competitive advantage

Optimised fraud risk management approaches should enable online merchants to accurately identify and filter out fraudulent transactions while providing good customers with a low-friction journey that helps to drive revenue growth.



2

Introduction by Forter



Introduction by Forter

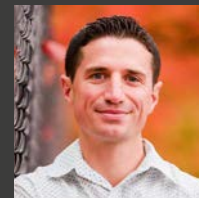
Across our global client base we see fraudsters continuing to adapt their methods and evolve new techniques to exploit system and process weaknesses for criminal purposes. Since Forter was founded over a decade ago, the nature and scale of eCommerce fraud has changed dramatically, with a growing diversity of risk types that merchants now need to understand and manage.

While eCommerce fraud might once have been considered to be synonymous with card payment fraud, the current threat landscape is far more diverse with account takeover fraud, refund fraud and policy abuse all becoming increasingly prevalent threat types. We should all expect the pace of change to remain high and new fraud threats to emerge as merchants develop new customer offerings, as alternative payment methods are introduced, as customer behaviours change and new technologies like AI are exploited by fraudsters.

The diverse nature of fraud threats means that online merchants need to have differentiated responses to different fraud risk scenarios that can effectively filter out fraud without unduly harming the experience for good customers. We often see merchants respond to fraud by deploying controls that either act as blunt instruments - preventing fraud but also harming good customer experience and revenue generation - or which require extensive manual intervention leading to high operational overheads. For us, fraud risk management is not just about blocking fraudulent transactions but also about effectively identifying good transactions to enable improved customer experience and drive revenue growth. Optimised fraud risk management strategies don't only prevent fraud losses and chargebacks, but can also act as profit drivers by reducing rates of cart abandonment and false declines.

Forter is a leader in eCommerce fraud prevention, processing over \$250 billion in online commerce transactions and protecting more than a billion consumers globally from credit card fraud, account takeover, identity theft and more. Forter enables online merchants to take a nuanced response to potential fraud threats, effectively filtering out fraud without harming good customer experience and avoiding legitimate customer payments being declined. Our platform leverages a deep understanding of more than 1.2bn online identities to accurately block fraud attempts while ensuring that legitimate customers get the seamless experience they deserve. Merchants that work with us become part of a fraud fighting consortium including the world's leading brands, with our sophisticated machine learning powered by shared intelligence that can react to rapidly changing threats.

Forter is very pleased to collaborate with PwC to bring the power of our data together with PwC's global network of eCommerce and fraud experts. PwC's work across global merchants and expertise in a wide range of other technologies means that they are well placed to advise merchants on how to optimise business processes to drive incremental revenue while effectively managing risk. This paper is one result of our partnership and combines analysis of Forter's data in combination with PwC's knowledge of merchants' operations to highlight ways to effectively manage fraud risk while optimising business processes to deliver incremental revenue.



Jeff Hallenbeck,
Head of Payments,
Forter

3

Understanding the complex nature of eCommerce fraud



Understanding the complex nature of eCommerce fraud

Fraudsters are highly agile and move quickly to exploit vulnerabilities across the customer checkout journey from account creation to returns. Changing merchant offerings and payment options, such as Buy Now Pay Later (BNPL), create new opportunities for fraud, requiring merchants to continuously evaluate and respond to potential fraud threats.

Fraudsters also quickly adopt new technologies for criminal purposes as shown, for example, by the 60% increase in Forter's detection of bots being used to attempt online purchases during 2023.¹ The increasing capabilities of generative AI tools and their widespread accessibility also has the potential to amplify the scale and sophistication of fraud attacks.

Notable threats include:



AI-generated image content:

Fraudsters using AI-generated images to socially engineer merchant employees. For example, using AI to create or manipulate images which depict a damaged item in order to obtain an illegitimate refund.



AI-enabled bot attacks:

Fraudsters harnessing AI to enhance the sophistication of bot attacks. This advancement enables them to circumvent security measures like CAPTCHA, thereby bypassing common customer account and payment security protocols.

Forter's data indicates that there has also been a significant rise in opportunistic frauds by otherwise legitimate customers exploiting promotion and refund policies for financial gain. Forter's consumer research reveals 56% of UK consumers confess to wardrobing (returning an item after use).² So-called 'friendly fraud' creates new challenges for merchants as customers that may carry out a refund fraud at one time may later return to being a 'good customer' another time. Decisions about whether to decline orders from these kinds of customers can be complex in the context of potential future purchasing. There is extensive content on social media platforms promoting fraudulent methods to acquire merchandise from online merchants, leading to a growing social acceptability of certain forms of eCommerce fraud further complicating merchant decision making.

1. Based on Forter's first-party data.






2. <https://resources.forter.com/resources/returns-abuse-infographic-jan24-uk%20>



Forter's consumer
research reveals

56%
of UK consumers
confess to wardrobing
(returning an item
after use).²

These developments lead to a highly complex fraud threat landscape for online merchants, with key risk areas including:

 <h3>Identity fraud</h3>	 <h3>Account takeover (ATO)</h3>	 <h3>Payment fraud</h3>	 <h3>Refund fraud</h3>	 <h3>Policy abuse</h3>
<p>Fraudsters create fake accounts to exploit new account opening offers or to use stolen payment methods. Merchants offering lines of credit or BNPL services are particularly vulnerable as fraudsters use these facilities to acquire goods without paying, leading to lost inventory and unpaid bills for merchants.</p>	<p>Fraudsters are increasingly using tools like bots and artificial intelligence (AI) to automate ATO attacks, enhancing their ability to hijack legitimate customer accounts using stolen login credentials. Social engineering techniques are also used by fraudsters to manipulate individuals into providing account login details. ATO attacks allow fraudsters to make purchases using saved payment details or to redeem account rewards like travel loyalty points.</p>	<p>Fraud involving stolen card details remains a key concern, with new payment methods introducing new payment fraud threats. For example, Forter's data indicates that there was a 24% increase in fraud attempts targeting digital wallets and BNPL services during the 2023 Black Friday weekend, indicating fraudsters' adaptability as merchants expand their payment options.³</p>	<p>With the implementation of Strong Customer Authentication (SCA) across Europe tightening payment fraud prevention, fraudsters have shifted focus to other points in the customer journey, particularly returns. Refund fraud encompasses various tactics, from falsely claiming non-delivery to returning counterfeit items, aiming to secure a refund while keeping the merchandise.</p>	<p>Fraudsters use various tactics, such as purchasing items and returning them after use or creating multiple accounts to exploit promotional offers. Merchants must effectively manage this threat to minimise losses without inconveniencing genuine customers, as overly strict policies can deter potential buyers. Forter's data indicates a concerning rise in the volume of fraud committed by 'good' customers with 18% of UK consumers admitting to opening multiple accounts to take advantage of promotions.⁴</p>

3. <https://www.forter.com/blog/black-friday-cyber-monday-the-good-the-bad-the-ugly/>

4. <https://resources.forter.com/resources/returns-abuse-infographic-jan24-uk%20>

Types of policy abuse



Wardrobing

Purchase items, wear them, and then return the items back to the store for a refund.

53%

of merchants have reported issues with renting and wardrobing.⁵



Free shipping abuse

Consumers return a high percentage of their orders back to the merchant for a variety of reasons.

30%

of users buy items with the intention of returning them, just to qualify for free shipping.⁵



New account opening abuse

The creation of multiple accounts to exploit promotional offers.

18%

of UK consumers admitting to opening multiple accounts to take advantage of promotions.⁶

5. <https://resources.forter.com/resources/hidden-costs-returns-abuse>

6. <https://resources.forter.com/resources/returns-abuse-infographic-jan24-uk%20>



4

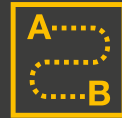
Effective fraud risk management for online merchants



Merchant priorities relating to fraud risk management



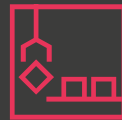
Optimising fraud controls to reduce friction



Driving a cross-organisation AI fraud response



Improving fraud analytics, MI and reporting



Increasing automation



Reducing friction and false declines



Leveraging third-party risk data to improve fraud detection accuracy



Outsourcing fraud operations

Effective fraud risk management for online merchants

Recognising that effective fraud risk management is a balancing act is critical to managing the overall impact on financial performance.

When assessing whether our clients have got the balance right, we consider the following key questions:

How effectively do current systems, processes and controls protect both your business and customers from both professional and opportunistic fraud?

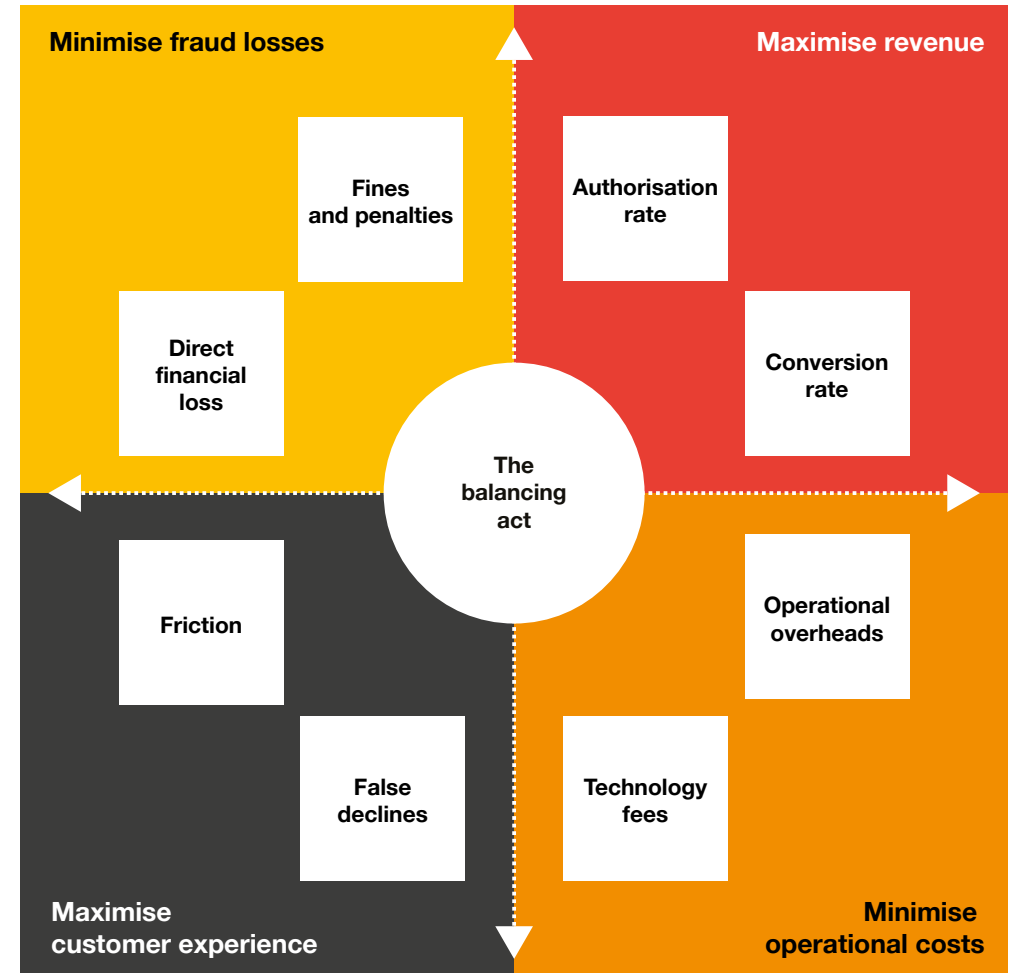
Are your marketing and product teams wasting their promotional budgets on customers which later turn out to be fraudulent?

Are there potential areas where efficiency gains can be achieved, reducing operational dependencies, by using new technologies or redesigning existing processes?

How many sales are you losing to not only fraud but also to cart abandonment and false declines?

By addressing these fundamental questions and adopting a holistic approach to fraud risk management, merchants can fortify their defences, safeguard their bottom line, and foster sustained growth in the dynamic landscape of eCommerce.

Figure 1 - The four-way eCommerce fraud balancing act



Merchants lose sales as a result of ineffective or poorly implemented fraud risk management approaches. Forter's global data indicates that for every £1 retailers are losing to fraud they are forfeiting £30 to false declines - meaning they were declining legitimate customer transactions because they mistook them for fraud.⁷

False declines not only impact revenue but also deter customers from future purchases with the brand. Forter's consumer research shows that 40% of shoppers abandon purchases after facing rejection,⁷ indicating a significant loss in potential sales, customer loyalty and brand reputation.

False declines can occur for a multitude of reasons. Forter's data shows that retailers often turn away new – but trustworthy – customers simply because they have never encountered them before. Forter's data indicates that false declines are typically 5 to 10 times higher than actual fraud.⁸ Merchants who rely on traditional rule based prevention methods often face challenges with higher false declines, as their rule sets struggle to adapt quickly enough to changing customer behaviour and shopping habits.

Today, merchants are focusing on data as a key enabler for a holistic approach to fraud prevention. By tapping into a variety of internal and external data sources, they're gaining deeper insights into customer identities. This enables them to more accurately assess customer transactions, reducing both fraud and the occurrence of false declines.

Leading merchants are adopting intelligence-based identity solutions that leverage understanding of shopper identities with machine learning models that enable more accurate risk assessment and reduction of false declines. These tools can spot trends and patterns with agility, automatically adapting to keep pace with changing fraud patterns. This can result in high fraud detection rates, which ultimately can convert to lower false declines.

Identity-based intelligence solutions combine customer data with machine learning algorithms to identify potential risk features and allow for accurate transaction evaluation. This valuable information is then shared with issuing banks, helping to minimise the risk of false declines. By providing issuers with a comprehensive set of data points, these solutions empower them to make informed decisions regarding 3DS exemptions.

Merchants adopting these progressive approaches typically experience an increase in acceptance rates. Issuers are reassured by the strengthened fraud controls implemented at the point of sale.

Every **£1** retailers are losing to fraud they are forfeiting **£30** to false declines.⁷



Case study:

Problems when fighting fraud

Business problem

This traditional UK-based merchant faced a series of payment fraud incidents leading to increasing chargebacks which began to impact overall profit and brand reputation.

In response to the uptick in fraud pressure, the merchant took the difficult decision to restrict what customers could order online and put all orders through manual agent review and 3DS challenge. This approach added a considerable level of friction into the merchant's customer journey as the merchant was unable to distinguish good trusted customer transactions from fraud attempts.

The merchant struggled to quantify what impact this approach was having on their sales channels making it hard to gauge the proportionality of its approach in the context of fraud prevention and lost sales.

7. <https://explore.forter.com/2023trustpremiumreport/p/1>

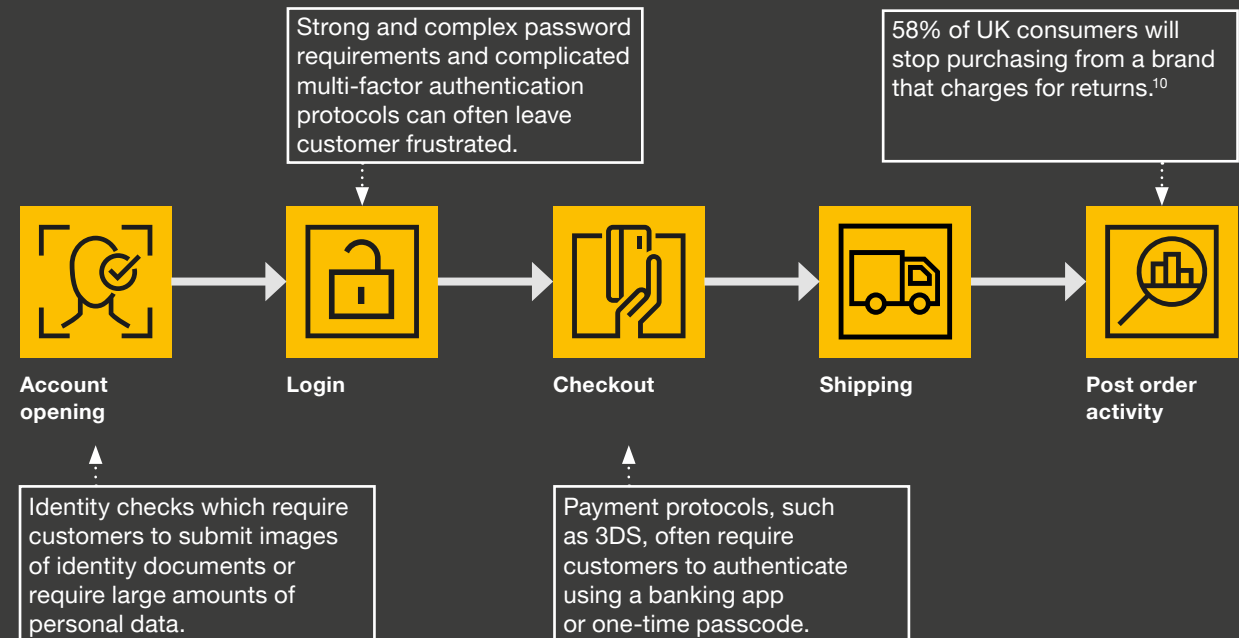
8. <https://www.forter.com/blog/winning-the-next-generation-of-holiday-shoppers/>

Is friction driving customers to your competitors?

Strong fraud prevention controls can often lead to higher frictions in customer journeys. While customers seek seamless and convenient checkout processes, poorly managed identity verification and fraud risk management procedures can create additional obstacles for the customer to navigate. Forter's consumer survey indicates that more than 75% of consumers will abandon their purchases if the checkout process is difficult / time consuming.⁹ This places merchants in a challenging position where they must strike a delicate balance between implementing effective fraud prevention measures while also accommodating evolving customer preferences.

Many merchants often focus solely on reducing fraud when managing their risk, overlooking the importance of addressing false declines and minimising customer friction. To effectively balance both business and customer needs, it's crucial for merchants to continually embrace data-driven process optimisation. This means tailoring strategies with both business requirements and customer experience in mind.

Figure 2 - Common areas of friction



9. <https://explore.forter.com/2023trustpremiumreport/p/1>

10. <https://resources.forter.com/resources/returns-abuse-infographic-jan24-uk%20>



Key considerations

Here are some key elements to consider:



Acquiring high-quality data:

Today, merchants are focusing on data as a key enabler for a holistic approach to fraud prevention. By tapping into a variety of internal and external data sources, they're gaining deeper insights into customer identities. This enables them to more accurately assess customer transactions, reducing both fraud and the occurrence of false declines.



Assessing risk:

By understanding who customers are, merchants accurately identify the risk they pose. By using data to obtain these insights merchants can complete these checks at speed with limited customer friction. Genuine customer transactions can be completed quickly with limited disruption whilst fraudulent transactions are stopped.



Sharing insights:

These valuable insights are shared with issuing banks to mitigate the risk of false declines. By providing issuers with a wealth of data points, these solutions empower them to make informed decisions regarding 3DS exemptions, reducing false declines without compromising fraud detection rates.



Improving technology:

Merchants can streamline processes by adopting integrated solutions capable of assessing risk, verifying customer identities, and sharing risk data all in a single solution. This approach enhances efficiency and effectiveness in fraud prevention efforts by consolidating the volume of controls in operation.

Payment Authentication: A Closer Look

Understanding 3DS

3D-Secure, commonly referred to as 3DS, is an additional layer of security for online credit and debit card transactions. 3DS has been designed to reduce unauthorised card use by requiring cardholders to authenticate themselves during the transaction process.

Many customers will experience 3DS when they transact online. The 3DS control will prompt the cardholder to enter a one-time passcode (sent to their email or mobile phone) or another form of authentication, such as verification using a mobile banking app, before the transaction can be successfully approved.

3DS is an important tool for verifying a cardholder's identity and reducing fraud. Although merchants in the UK and Europe have been accustomed to 3DS since the introduction of PSD2, how merchants adopt and continuously manage their approach to 3DS still requires careful consideration.

The price of 3DS

Merchants not only stop fraud with blanket fraud risk management strategies but often negatively impact the genuine customer experience through false-declines and friction. Forter's data indicates unnecessary friction applied on the checkout journey can result in good customers abandoning cart in favour of a smoother checkout experience.

But how are some merchants using 3DS to attract customers whilst others are falling foul to the 3DS pitfalls?

Understanding 3DS

19%

of 3DS attempts fail in the UK.¹¹

16%

of UK shoppers abandon their cart after being presented with 3DS.¹²

30%

of 3DS attempts fail in Europe.¹³

11%

of 3DS challenges are abandoned without attempt.¹⁴

11. <https://www.forter.com/blog/the-cost-of-3ds-how-blanket-strategies-affect-good-customers/>

12. Based on Forter's Payment Data

13. <https://www.forter.com/blog/when-and-how-to-properly-use-3ds2/>

14. Based on Forter's payment data.

Getting the balance right

By taking an informed and well considered approach to how 3DS is implemented can drive value. We often see leading merchants focus on two key areas:

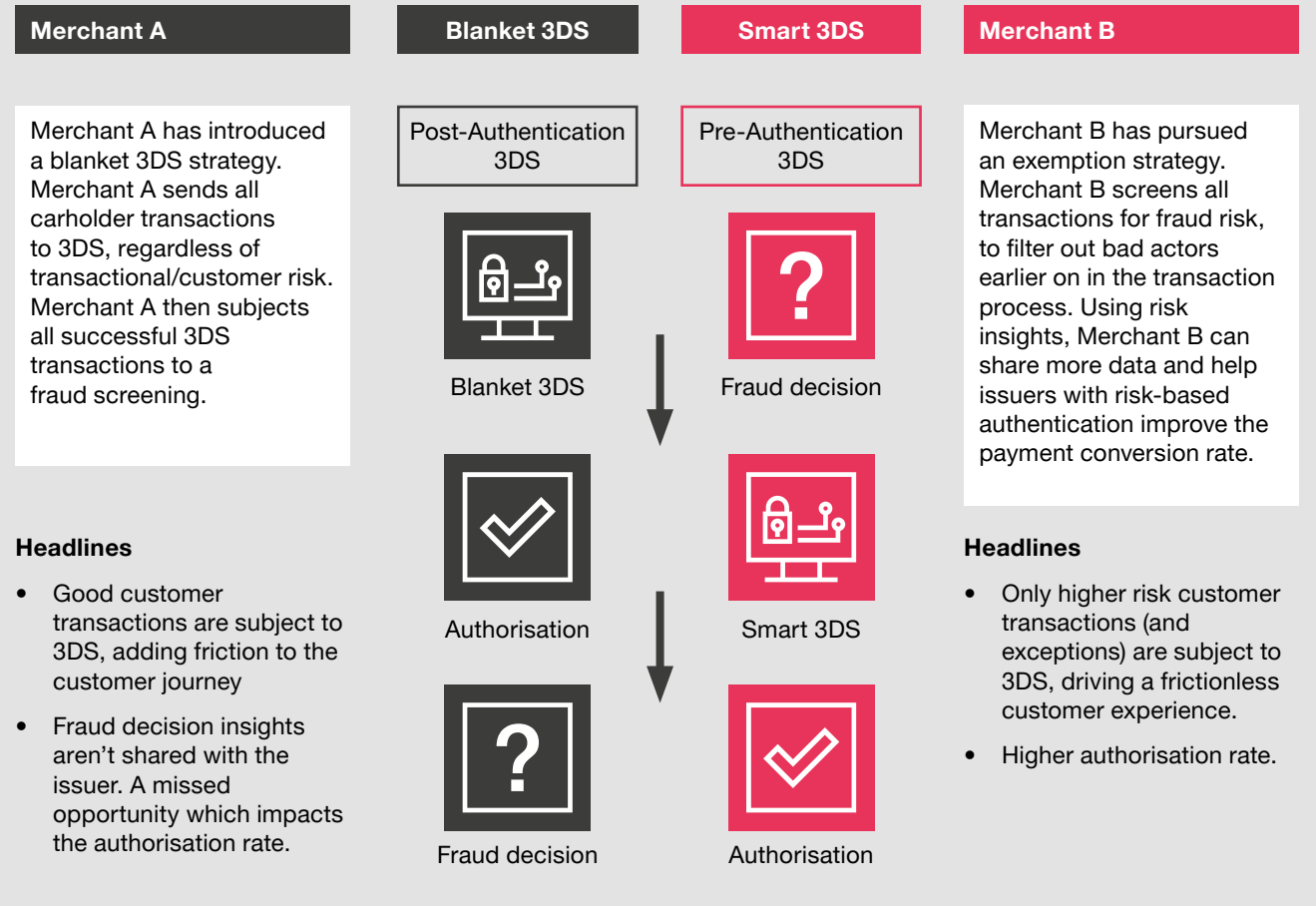
Orchestration:

How is 3DS integrated into the payment journey to achieve a slick, seamless and ultimately safe experience for customers?

Optimisation:

What data points are being collected throughout the payment journey to support smart 3DS decision making? Are exemptions being used by the merchant to reduce the number of times trusted cardholders are required to authenticate? Are additional data points being shared with issuing banks to improve risk decisioning?

Transitioning to smart 3DS



Are you paying a high price to prevent fraud?

If you are looking to focus on understanding the effectiveness of your current fraud risk strategies, increase the impact of your fraud investments and optimise your processes to improve your margin, understanding the true cost of fraud is vital.

Calculating your true cost of fraud

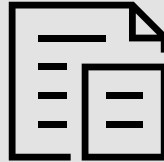
Direct financial losses



Cost of your fraud control infrastructure



Hidden costs of fraud prevention



Case study:

Health and wellness merchant reduces fraud and improves the customer experience using Forter.

Business problem

The merchant encountered challenges distinguishing authentic customers from fraudulent ones, leading to an escalating chargeback rate, penalties from monitoring schemes, and unwarranted declines.

Additionally, the merchant faced operational constraints as their team spent much of their time investigating each transaction.

This outdated approach not only hindered sales and revenue but also compromised the overall customer experience.

Achievement

99.95%
approval rate.¹⁵

90%
decrease in
monthly chargebacks.¹⁵

\$300,000
in penalties with Visa
and Mastercard avoided.¹⁵

15. <https://resources.forter.com/resources/case-study-nutrisystem?xs=437761#page=1>

Direct financial loss – Chargebacks and more

Many merchants underestimate the true cost of chargebacks. Chargebacks are not just about the cost of paying back a chargeback claim, in reality they cost a business much more than this. Sanctions from the card scheme and additional fees from acquirers, and the operational burden of investigating chargeback claims are some of the associated costs which are often overlooked.

Chargebacks are important for merchants to monitor and minimise, but they aren't the only piece of the puzzle. In recent years, there has been a worrying rise in customers exploiting promotions and refund policies for personal gain. These fraud threats can result in significant financial losses for merchants, ultimately reducing revenue and wasting internal resources.

Merchants who overlook the comprehensive scope of financial loss are susceptible to making ill-informed business decisions that fail to address the most imminent threats. Next time you're reviewing your fraud metrics, ask yourself are all fraud losses being considered?



Cost of your fraud control infrastructure - Manual intervention

Managing fraud risk goes beyond just using technology. It's a big operational challenge for merchants. Often, they rely on manual reviews, which can be a heavy burden. This traditional approach to fraud detection involves significant operational support and, in some cases, requires teams to work round the clock to minimise the impact on customer orders.

Often we see merchants underestimating the true operational costs on their bottom line. With a narrow focus on manual order reviewers, many overlook how fraud risk management impacts over operational teams. We have included an example operational flowchart below, to support you in thinking about your own operational response to fraud:



Knowing the real cost of managing fraud cases is crucial. Yet, many merchants underestimate how much fraud affects their profits. What are leading merchants focusing on when they think about fraud operations?

Cost to serve

Cost-to-service analysis helps businesses calculate the real cost of managing fraud cases. Its goal is to grasp the full financial impact of handling fraud, pinpointing areas where merchants are losing money. This insight supports smarter decision-making allowing merchants to spot unprofitable areas to target with optimisation initiatives.

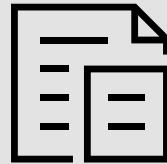
Double handling rates

Double handling occurs where inefficiencies in operations cause cases (like fraud remediation work) to be reopened and dealt with again. This can be due to issues like inadequate training, technology problems, or disorganised workflows. Merchants who do not track case re-open rates miss out on opportunities to save costs and streamline operations, ultimately improving the customer experience.

Hidden costs of fraud prevention

The consequences of false declines and unnecessary friction go beyond the mere financial loss of a failed transaction. They often result in customers abandoning their carts, causing a loss in customer lifetime value (CLV) and damaging the company’s reputation.

This reputational damage can be exacerbated by social media platforms and eCommerce review sites. Similar to a domino effect, the persistence of false declines and friction can continue to harm your bottom line long after the initial incident. Therefore, it’s crucial for merchants not only to quantify these metrics but also to report on them periodically to gain actionable insights for improving strategic decision-making.



Case study:

How a global online travel agency reduced their dependency on manual process for fraud prevention using Forter.¹

Business problem

The online travel agency was using a third-party solution which relied on manual reviews which resulted in an operational backlog (5-minute review on average).

Achievement

100%
reduction in manual reviews.¹⁶

The manual reviews added unwanted friction to the company’s otherwise streamlined customer experience. During this process some customers were phoned for verification or required to send in a photo of their passport.

97%
payment approval rate.¹⁶

The online travel agency needed a solution which could support business growth, reduce operational costs and customer friction without compromising their fraud rate.

40%
fraud chargeback improvement.¹⁶

16. <https://www.forter.com/customers/kiwi/>

5

Optimising fraud risk management practices



Optimising fraud risk management practices

Characteristics	Processes are ad hoc and reactive.	Heavy reliance on manual verification processes and 'paper-based' documentation - often reactively reviewing orders post-fulfillment.	Adoption of rule-based systems to automate some fraud detection/prevention processes. Commonly supported by some manual intervention.	Technologies solutions leveraging machine learning enable identification of fraud by analysing patterns and anomalies in near real-time.	Integration of fraud prevention technology across the end-to-end omni channel ecosystem. Platform enables proactive and agile responses to changing threat patterns.
Technology	No primary fraud prevention capability.	Spreadsheets used as the primary tool to examine orders. Basic transaction data used during fraud detection activities. Prevention mechanisms are reactive and largely operational.	Transaction monitoring solution which uses basic transaction/customer data and pre-defined rules. Rules are typically reactive and hard to scale, creating high rates of false positives over time.	Behavioural, anomaly and predictive modelling is used to identify unusual activity. Data is enriched with alternative sources such as device fingerprinting, behavioural biometrics and additional risk data from consortium networks. Significant reliance on automated processes to reduce manual prevention activities.	Artificial intelligence (AI) driven predictive modelling utilising large and complex datasets which incorporates network risk data. Technology is embedded across the end-to-end omnichannel checkout journey to holistically manage customer risk with minimal manual intervention.
Analytics and reporting	No fraud analytics or reporting.	Little to no data analytics. Business uses manual processes for data aggregation. Basic fraud KPI reporting, largely focused on chargeback data received from banks.	Some data analytics and management capabilities. Fraud data siloed and not integrated with other data sources. Developing KPI reporting which focuses on financial losses and rejected orders.	Big data analytics is used for decision making. Cross-organisational approach to data integration and accessibility. Robust KPI and KRI reporting which frequently produced detailing financial losses, customer impact metrics, control indicators and overall risk management performance.	Sophisticated real-time data analytics which is used across the overall fraud management framework. Advanced KPI and KRI reporting accessible by all business units. Accessible metrics across the organisation drive strategic advancements enterprise-wide.
	1) Non existent	2) Manual verification	3) Rule-based systems and some automation	4) Machine learning, real time monitoring and advanced analytics	5) Integrated omni channel infrastructure and agile technologies

Using PwC's industry insights, we have created a fraud risk management maturity model which focuses on technology and data analytics. This maturity model defines the different stages of evolution an merchant can go through when developing an approach to fraud risk management.

It serves as a tool for merchants to assess their current status and identify the next steps for enhancing their capabilities, taking into account the broader industry.



Case study:

Case study: Global apparel and footwear merchant improves approvals and reduces chargebacks using Forter.¹

Business problem

The merchant faced a rise in online orders, which increased fraud rates and led to revenue loss. Adding to the challenge was the merchant’s reliance on an outdated and unscalable manual order review process.

To address this situation, the merchant sought a solution to support business growth, cut operational costs, and reduce customer friction without compromising the existing fraud rate. The goal was to enhance efficiency and effectiveness while navigating the complexities of the evolving online landscape.

Achievement



Elimination of manual reviews.¹⁷



12.6% increase in approvals.¹⁷



Chargeback rate reduced to 0.02%¹⁷

17. <https://resources.forter.com/resources/case-study-reebok>



6

Considerations for the industry



Considerations for the industry

Optimisation has emerged as a strategic area of focus for leading merchants. Merchants that get the right blend of technology and data can control costs, drive sales, minimise customer friction all whilst effectively mitigating fraud.

Explore holistic fraud monitoring capabilities

We often see merchants invest in fraud risk management capabilities comprising both operational and technological controls. However, many merchants lack a comprehensive view of fraud risk across their end-to-end checkout journey and control infrastructure. Fraud risk is often viewed through the narrow lens of chargebacks with a significant focus on payment fraud, and merchants often fail to quantify other associated fraud impacts such as operating costs and customer experience. By failing to develop a holistic view of fraud, merchants will struggle to introduce strategies that effectively protect both customers, their business and revenue.

Leading merchants often have robust fraud risk monitoring programmes in place which not only quantify the direct financial impact of fraud (e.g. chargebacks) but a broad spectrum of key risk indicators (KPIs) covering operational costs, customer experience and control performance metrics. By taking this approach, business decision makers are empowered to make well-informed, cost-conscious, strategic decisions which promote efficient allocation of internal resources to prevent fraud whilst putting the customer first.

Put the customer at the centre of your fraud risk management strategies

Historically, merchants have introduced fraud controls at the cost of the customer experience. By broadly applying controls, such as MFA, merchants are adding unnecessary friction to their checkout journeys which are driving cart abandonment and false declines. Leading merchants are adopting customer-centric approaches that seek to balance fraud prevention with customer experience.

They are doing this by:

- **Using enhanced risk data:** By leveraging enhanced risk data, such as device, location, behavioural and network data, merchants are able to accurately differentiate legitimate customers from fraudsters in near real-time.
- **Dynamically applying friction:** Leading merchants are using these insights to dynamically apply friction across their fraud prevention strategies. This means genuine customers can enjoy a frictionless shopping experience, whilst higher risk transactions are subject to identity verification protocols.



Considerations for the industry

Develop your use of automation

eCommerce fraud threats change rapidly and well understood fraud types like card-not-present fraud are being joined by new threat types such as triangulation fraud and policy abuse. With advancements in artificial intelligence technologies, merchants are seeing increases in the scale and sophistication of fraud attacks. Typically these attacks require operational resources to remediate, requiring both analysts to update rule based systems and reviewers to triage high risk order referrals.

Leading merchants are revolutionising their fraud detection processes using tools such as machine learning and artificial intelligence to automate their primary fraud controls.

Improve your cross-organisational ways of working

To effectively protect your business from the impacts of fraud, a whole organisational response is needed, bringing together fraud teams and product teams. Typically when we work with merchants, it is apparent that fraud risk management activities and reporting have been performed on a siloed basis.

As part of the development of the forward-looking strategy, merchants should consider how to embed fraud risk management activities within the end-to-end business and product lifecycle, and provide visibility of fraud trends and issues to drive the right level of cross-organisational investment.



7

PwC
contact details



PwC contact details



Casey Pozarowszczyk

Manager | Forensics

PwC UK

casey.pozarowszczyk@pwc.com



Tobias Beal

Senior Manager | Forensics

PwC UK

tobias.beal@pwc.com



Harry Holdstock

Partner | Financial crime

PwC UK

harry.g.holdstock@pwc.com



Thank you

[pwc.co.uk](https://www.pwc.co.uk)

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2024 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.legal entity.

RITM16130293

